UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/044,432	01/11/2002	Jason Robert Almeida	RPS9 2001 0091 US1	8540

56102 7590 08/02/2006

IBM (RPS-BLF)
c/o BIGGERS & OHANIAN, LLP
P.O. BOX 1469
AUSTIN, TX 78767-1469

EXAMINER	
CERVETTI, DAVID GARCIA	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 08/02/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/044,432
Filing Date: January 11, 2002
Appellant(s): ALMEIDA, JASON ROBERT

Joseph P. Lally, Reg. No. 38,947
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed June 12, 2006 appealing from the Office action mailed October 12, 2005.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

A statement identifying the related appeals and interferences which will directly affect or be directly affected by or have a bearing on the decision in the pending appeal is contained in the brief.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,141,756	BRIGHT et al. (Bright)	10-2000
5,968,174	HUGHES (Hughes)	10-1999
6,151,676	CUCCIA et al. (Cuccia)	11-2000

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-2, 4-5, 9-10, 12-13, 17-18, and 20-21 are rejected under 35 U.S.C. 102(b) as being anticipated by Bright.

Regarding claim 1, Bright teaches

- a computer program product comprising processor executable instructions for programming a non-volatile storage element in a data processing system, the instructions being stored on a computer readable medium (column 1, lines 60-67, column 2, lines 1-26, column 5, lines 24-32), comprising:
- computer code means for encrypting a digital signature using a first encryption key (column 3, lines 40-57);
- computer code means for passing the encrypted signature to a kernel routine (column 3, lines 58-67, column 4, lines 1-13);
- computer code means, responsive to successfully decrypting the encrypted signature using a second encryption key, for transitioning the

data processing system from a protected-mode to a real-mode (column 4, lines 14-32); and

- real-mode computer code means for flash programming the non-volatile storage element (column 5, lines 1-13).

Regarding claim 2, Bright teaches wherein the code means for encrypting the digital signature is non-privileged code.

Regarding claim 4, Bright teaches wherein the first encryption key is a private key and the second encryption key is a public key, wherein the public key and private key are generated from a common algorithm.

Regarding claim 5, Bright teaches further comprising code means for generating the digital signature, wherein the digital signature includes information that is indicative of the data processing system (column 3, lines 46-57).

Regarding claim 9, Bright teaches

- a data processing system including at least one processor, memory, and input means connected to a common bus, wherein the system memory contains at least a portion of a sequence of computer executable instructions for programming a non-volatile storage element of the data processing system (column 1, lines 60-67, column 2, lines 1-26, column 5, lines 24-32), the instructions comprising:
- computer code means for encrypting a digital signature using a first encryption key (column 3, lines 40-57);

- computer code means for passing the encrypted signature to a kernel routine (column 3, lines 58-67, column 4, lines 1-13);
- computer code means, responsive to successfully decrypting the encrypted signature using a second encryption key, for transitioning the data processing system from a protected-mode to a real-mode (column 4, lines 14-32); and
- real-mode computer code means for flash programming the non-volatile storage element (column 5, lines 1-13).

Regarding claim 10, Bright teaches wherein the code means for encrypting the digital signature is non-privileged code.

Regarding claim 12, Bright teaches wherein the first encryption key is a private key and the second encryption key is a public key, wherein the public key and private key are generated from a common algorithm.

Regarding claim 13, Bright teaches further comprising code means for generating the digital signature, wherein the digital signature includes information that is indicative of the data processing system (column 3, lines 46-57).

Regarding claim 17, Bright teaches

- a method of programming a non-volatile storage element in a data processing system (column 1, lines 60-67, column 2, lines 1-26, column 5, lines 24-32), comprising:
- encrypting a digital signature using a first encryption key (column 3, lines 40-57); passing the encrypted signature to a kernel code routine (column

3, lines 58-67, column 4, lines 1-13); responsive to successfully decrypting the encrypted signature using a second encryption key, transitioning the data processing system from a protected-mode to a real-mode with the kernel code routine (column 4, lines 14-32); and flash programming the non-volatile storage element in real mode (column 5, lines 1-13).

Regarding claim 18, Bright teaches wherein encrypting the digital signature comprises encrypting the digital signature with non-privileged code.

Regarding claim 20, Bright teaches wherein the first encryption key is a private key and the second encryption key is a public key, wherein the public key and private key are generated from a common algorithm.

Regarding claim 21, Bright teaches further comprising generating the digital signature, wherein the digital signature includes information that is indicative of the data processing system (column 3, lines 46-57).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 3, 11, and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bright as applied to claims 2, 10, and 18 respectively above, and further in view of Hughes.

Regarding claims 3 and 11, Bright teaches the limitations as set forth under claims 2 and 10 respectively above.

Bright does not disclose expressly wherein the code means for passing the encrypted signature to the kernel routine comprises code means for executing a system call from the non-privileged code and passing the signature as a parameter of the system call.

However, Hughes teaches wherein the code means for passing the encrypted signature to the kernel routine comprises code means for executing a system call from the non-privileged code and passing the signature as a parameter of the system call (column 7, lines 28-32).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to execute a system call and pass a parameter to a system call.

One of ordinary skill in the art would have been motivated to do so because it is well known in the art to execute a system call from the non-privileged mode and passing a value as a parameter to a system call.

Regarding claim 19, Bright teaches the limitations as set forth under claim 18 above.

Bright does not disclose expressly wherein passing the encrypted signature to the kernel routine comprises executing a system call from the non-privileged code and passing the signature as a parameter of the system call.

However, Hughes teaches wherein passing the encrypted signature to the kernel routine comprises executing a system call from the non-privileged code and passing the signature as a parameter of the system call (column 7, lines 28-32).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to execute a system call and pass a parameter to a system call.

One of ordinary skill in the art would have been motivated to do so because it is well known in the art to execute a system call from the non-privileged mode and passing a value as a parameter to a system call.

Claims 6-7, 14-15, and 22-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bright as applied to claims 5, 13, and 21 respectively above, and further in view of Cuccia.

Regarding claims 6, 14, and 22, Bright teaches the limitations as set forth under claims 5, 13, and 21 respectively above.

Bright does not disclose expressly wherein the digital signature is generated based at least in part upon dynamic information.

However, Cuccia teaches wherein the digital signature is generated based at least in part upon dynamic information (column 8, lines 13-20).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to generate a digital signature from dynamic information.

One of ordinary skill in the art would have been motivated to perform such a modification to provide a way to authenticate a user (Cuccia, column 2, lines 34-40).

Regarding claims 7, 15, and 23, the combination of Bright and Cuccia teaches the limitations as set forth under claims 6, 14, and 22 respectively above.

Furthermore, Bright teaches wherein the digital signature is generated at least in part based further upon information including a corresponding hostname and process ID (column 3, lines 50-52, a hash function).

Claims 8, 16, and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bright as applied to claims 1, 9, and 17 respectively above, and further in view of Cuccia.

Regarding claims 8, 16, and 24, Bright teaches the limitations as set forth under claims 1, 9, and 17 respectively above.

Bright does not disclose expressly further comprising code means for generating a random number as the digital signature.

However, Cuccia teaches further comprising code means for generating a random number as the digital signature (column 8, lines 13-20).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to generate a random number as the digital signature.

One of ordinary skill in the art would have been motivated to perform such a modification to provide a way to authenticate a user (Cuccia, column 2, lines 34-40).

(10) Response to Argument

Examiner respectfully submits that the argument presented in the Final Office Action, was meant to be an inherency argument, since the prior art anticipates the claimed language.

Regarding Appellant's assertion that Bright does not disclose transitioning from protected to real modes or a kernel routine, Examiner respectfully disagrees with Appellant.

Bright discloses two modes, a mode where sensitive processing occurs (bootstrap mode), which corresponds to Applicant's "protected mode", and transition to execution of program upon successful decryption/validation/authentication, which is inherent, real mode (column 1, lines 10-45).

Examiner further refers to figure 3, steps 301-315 which correspond to "protected mode", perform decryption, and at step 317 executes the program which is executing in a non-secure mode, which corresponds to Applicant's "real mode", an inherency of the system (column 3, line 58, to column 5, line 12). The fact that Bright does not use the words "real mode" and "protected mode" carry no relevance since Bright's

elements/modes provide a mode to perform validation and upon successful validation/authentication transition a system from mode A (bootstrap) to a mode B (column 2, lines 3-26, 45-67).

Bright further provides the teachings for transitioning a system from bootstrap mode to another mode upon successful authentication using encryption/decryption techniques (column 1, lines 10-45).

Bright further discloses the bootstrap mode performs the authentication and allows the processor to execute the program (a second mode, different from the bootstrap mode, column 3, lines 57-67, column 6, claim 22).

Bright's bootstrap mode performs at the kernel level, thus anticipating "passing the encrypted signature to a kernel routine" (column 4, lines 14-55).

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

David Garcia Cervetti

July 28, 2006

Conferees

Gilberto Barron

Supervisory Examiner

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Kambiz Zand

Primary Examiner